JURISGRADIBUS-*Articles* **ISSN: 2585-3554**

April-June, vol. 2, n. 1, 2023 Article 2

INTERNET COOKIES IN EUROPEAN UNION (EU) LAW

Mark Davis

DOI:10.5281/zenodo.8130997

INTERNET COOKIES IN EUROPEAN UNION (EU) LAW

Mark Davis, Ph.D in European Union Law, UK

Abstract: The present paper attempted to analyze the evolution of the use of internet or HTTP cookies through a more concrete discourse on personal data and national security in the practice of the European Union (EU) law. The analysis is oriented towards the transfer of personal data also outside the EU and above all in the United States. What kind of protection do we have? What are the problems inherent in data transfer? These are some of the topics under examination above all to the persistent critical issues that such a transfer entails the risk of a rejection by the CJEU. The paper ends up with the contributions and critical aspects the new ePrivacy regulation provides for.

Keywords: internet cookies; cookie walls; dark patterns; google analytics; data transfer; European Union law; General Data Protection Regulation; consent; ePrivacy Regulation; metadata.

INTRODUCTION

Internet cookies, web, social networks, Youtube, Facebook, IP address, etc. are some of the applications used in recent years especially by young people as an effective consequence of the continuous development of information technology (Schwarz, 2001). What makes us feel more interested was the connection of technology with personal data and personal protection and above all the last discourse on internet cookies as an organ of processing, collection and sharing of personal data given that the user is informed about it.

The information and communication society is a type of community

that makes knowledge and its sharing the key elements around which to develop the activities characterizing social and economic life. The growing possibility offered by technological supports to easily exchange contents of various types, overcoming the traditional space-time barriers, has, over the years, deeply innovated the traditional way of understanding economic activity, the methods of interaction between the associates and the provision of public services that are now fully nourished by the interactivity, versatility, speed and globality of the services offered by the network (Liakopoulos, 2020).

Internet cookies are digital microfiles that allow a device to be associated, including the IP address, with the behavioral choices of a user. Internet cookies are used by web applications on the server side to store and retrieve long-term information on the client side. Immediately a jurist feels happy because this will be a hunt for pedophiles, prohibited pornography, etc. but it's not that easy. The information of an encoded nature through internet cookies includes personal data that are part of the so-called active identifiers where, through actionable tools, they allow each user to refuse their consent, thus avoiding the tracking of proceeding in a direct way to remove the internet cookies that are stored on their own device. Such passive identifiers do not include the storage of information or access to the user's device but only the reading of its configuration which remains fully available to the user.

Internet cookies include proprietary or first-party cookies when they are installed, deleted and directly modified by the site visited and those of third parties which are created by other owners' sites and content they view on the web page of the site they are viewing through the own visit to the internet. These are divided into technical, analytical and

profiling internet cookies. Technical cookies are used for navigation on each website and allow full use of all the features of the site itself. This type of internet cookie requires computer authentication, session monitoring and storage of specific information of the person/s who visit each site. Analytical cookies have the objective of collecting information from websites relating to user access, such as the number of visitors, the duration of their stay on the site as well as the sites they visit, i.e. the web audience measurement. As far as profiling cookies are concerned, they are used to monitor and profile the related users who, during navigation, study their own movements and web consultation and consumption habits in order to measure the effectiveness of the advertising message as well as to conform the type and methods of the services rendered to the behavior of the related users as an object of observation.

Internet cookies are also used for commercial reasons, above all to proceed with the profiling of internet users. AdTech is mentioned, i.e. advertising technology where its origin is largely due to the continuous development of internet cookies that dates back to 1993 (Shah, Kesan, 2004; Turner, Johnson, 2017; Edwards, 2018; Edwards, 2019; Hallinan, Leenes, Gutwirth, 2020)[1]. Advertising is based on the content of the site where the ad appears. Behavioral advertising based on data collection where, through cookies, the browsing activity of a computer user and online behavior provides tailored ads are based on one's interests.

As can be understood, the types of internet cookies except the technical ones are likely to have a significant impact on the privacy of Internet users. The use applied makes individual users identifiable also through

1According to Edwards: "(...) the cookies technology was the most innovative feature and one that would forever alter the web (...)".

the collection of anonymous data such as IP addresses.
The European legal framework is not limited to the use of internet cookies but also to the transfer of personal data from the EU to third countries especially in the United States, as well as to subordinate transfers and compliance with European standards regarding the use of internet cookies and ePrivacy.

TOWARDS AN EU COOKIE LAW

The main instrument of cookie law by the side of EU was the Directive 2002/58/EC (Feiler, 2010)[2] on privacy and electronic communications, the so-called ePrivacy Directive[3] later amended by Directive 2009/136/EC (Sauter, 2014)[4]. Among its main objectives was the guarantee of confidentiality of electronic order communications as well as the confidentiality of communications in general that have to do with personal data. The user must consent to the use by the manager of an internet site of cookies and the storage of access data on his computer (Article 5.3) (Feiler, 2010)[5]. As an exception to the rule of consent is that cookies of a technical nature, i.e. the internet cookies

2Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63, date of end of validity 8 April 2014.

3Directive cookies law.

4Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58 /EC relating to the processing of personal data and the protection of privacy in the electronic communications sector and to Regulation (EC) no. 2006/2004 on cooperation between the national authorities responsible for the enforcement of consumer protection legislation.

5Art. 5.3 of the Directive ePrivacy.

used, carry out the transmission of a communication over an electronic communications network, or to the strictly necessary extent to provide an information society service explicitly requested by the subscriber or by the user[6]. After the changes introduced in 2009 we have to do with a circle, rectius more general picture of the European reform on electronic communications networks and services. Internet cookies make the transition from an opt-out model to an opt-in one. Then the transition from the opt-out where it was sufficient to allow the user's refusal to install opt-in cookies requires the user's consent for any use that is not connected with the service rendered.

Consent as a prerequisite for the processing of personal data is again regulated in a clearer and more detailed way than in the past through Regulation 2016/679 (GDPR) (De Hert, Papakonstantinou, 2012; Mantelero, 2012; Van Alsenoy, 2017b; Deac, 2018; Wulf, Seizov, 2022)[7] and from Directive 2016/680/EU (Caruana, 2017)[8] concerning the

6"Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only permitted on condition that the subscriber or user concerned is been informed clearly and fully, inter alia, of the purposes of the processing in accordance with Directive 95/46/EC and that he is given the possibility to refuse such processing by the controller".

7Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1-88.

8Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89-131.

sectors of prevention, contrast and repression of crimes. The dual purpose that animates the entire regulatory system immediately emerges, i.e. the will not to lose the extraordinary evolutionary path represented by the new digital technologies, now having the strategic character of growth on a global level of modern advanced societies and at the same time configuring the need for this evolution without compromising the core of the fundamental rights recognized to the single individual and consequently the user who is an expression and legitimization of the European constitutional traditions and of the citizens of the EU.

Remaining on the topic and especially on the relationship between Regulation (EU) 2016/679 and Directive (EU) 2016/680 we can say that it is governed by recital 11 of the Directive and recital 19 of the GDPR Regulation. It is thus established that the data is collected by private or public subjects and used for purposes other than those of prevention, investigation and detection and prosecution of crimes, by applying the GDPR Regulation. On the other hand, according to the recital 19, the competent authorities pursuant to Directive (EU) 2016/680 are called upon to perform functions aimed in a manner necessary for the prosecution of crimes and the execution of criminal sanctions. In any case, the Directive is applied whenever private parties collect and process personal data according to the objectives established by Article 1, par. 1 and/or on behalf of law enforcement authorities (Van Alsenoy, 2017a; Purtova, 2018)[9]. In the latter cases, the authorities act as data

9An example of private actors acting, however, on behalf of the law enforcement authority, is represented by analysis centers / laboratories that analyze the evidence gathered in relation to a specific criminal offense and whose results are then transmitted to the police authorities for the purpose that they can be used in preliminary investigations or attached to the records of the process.

controllers and private actors pose as data processors. The hypotheses under investigation must be governed "(...) by a contract or other legal act and by the provisions applicable to data controllers pursuant to this Directive (...)" (Van Alsenoy, 2017a). It can be assumed that while the GDPR Regulation applies in the initial phase of data collection, subsequently processed for law enforcement reasons they are governed by Directive (EU) 2016/680. What is the exact moment from which one or the other legislation will apply? Neither the Regulation nor the Directive seem to have provided an exhaustive and concrete answer, therefore an area of uncertainty persists in which in fact both one and the other regulatory source could apply interchangeably.

The proposed consent by the GDPR was a manifestation of free, specific[10] will dealing only with the data subject, and speaking to user identification[11]. This consent to the processing:

> "(...) must be given for one or more specific purposes pursuant to Article 6 (...). This is expressed by means of an unequivocal positive deed with which the interested party demonstrates the free, specific, informed and unequivocal intention to accept the processing of personal data concerning him (...)"[12].

The express consent can be revoked at any time[13]. And in the event that "(...) the processing has multiple purposes, consent should be given for all of these (...)"[14]. This is an application provided for the use of internet cookies.

Internet cookies have as a requisite the transparent and concise modality of cookie banners, i.e. the warnings that must be shown to

10Art. 13 GDPR.
11Art. 4 GDPR.
12Recital 32 GDPR.
13Art. 7 GDPR.
14Recital 32 GDPR.

users when a user accesses a website, arriving at information of the presence of any internet cookies, of their rights and ask for installation consent[15]. According to Regulation 2016/278[16], online data controllers continue to use preselection boxes as a type of default setting, thus inducing users to accept cookie devices of first or third parties. This practice was also commented by the Court of Justice of the European Union (CJEU) in case Planet stating that in no uncertain terms the only valid form of consent for the processing of user data is express consent, i.e. the one that lends actively and specifically the pre-selection of the boxes to express consent to the use of internet cookies. Users must also be informed about the duration of internet cookies and the possibility that third parties access their data, since both profiles constitute specific methods of processing personal data (Wiedemann, 2020)[17]. An active consent on the part of the interested party was confirmed by the judges of Luxembourg through the Orange România SA case[18].

TRANSFER OF PERSONAL DATA AND INTERNET COOKIES OUTSIDE THE EU CONTEXT

One of the goals of the internet was its global use without limited to

15Art. 5.1 lett. a and art. 12 GDPR.

16Commission Implementing Regulation (EU) 2016/278 of 26 February 2016 repealing the definitive anti-dumping duty imposed on imports of certain iron or steel fasteners originating in the People's Republic of China, as extended to imports of certain iron or steel fasteners consigned from Malaysia, whether declared as originating in Malaysia or not C/2016/1316, OJ L 52, 27.2.2016, p. 24-26.

17C-673/17, Planet49 of 21 March 2019, ECLI:EU:C:2019:246, published in the electronic Reports of the cases.

18CJEU, C-61/19, Orange România SA v. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) of 11 November 2020, ECLI:EU:C:2020:901, not yet published.

state regulation barriers. What was most interesting was that personal data are transferred outside the EU context. Cross-border transfers are essential for the development of international trade (Burri, Schär, 2016)[19] and the related flows constitute the fastest growing trade in the EU, as in the US where the circumstance of European legislation cannot set standards of protection with a consequence the risk of a formalistic approach not finding a single solution. As early as 1998, the European Commission spoke for the categories of transfers that represent a threat to privacy with greater attention: "(...) to the behavior of data collection by means of new technologies in particularly hidden or clandestine (e.g. the so-called Internet "cookies" (...)"[20].

Later Regulation 2016/278, it took a position through Chapter V (Articles 44-50) regarding the transfer of personal data to third countries and international organizations where it was decided to adopt ad hoc mechanisms to guarantee the established transfer to an adequate level of protection[21]. Within this context, the subject of data transfer to countries such as the US is a topic of continuous discussion with many legal, technical and political gaps (Whitman, 2004; Glass, 2010; Flor, 2021).

Within this context we recall the agreements between US and EU, the Safe Harbor and the Privacy Shield[22] and the decisions that are adequate according to the pre-established positions of the EC and

19Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (see preamble 56).

20European Commission, Working Party "Protection of natural persons with regard to the processing of personal data" DG XV D/5025/98 WP 12.

21Recital 101 GDPR.

22Decision of European Commission n. 1250/2016/EC of 12 July 2016.

declared through the Schrems case (Scheck, 2012; Lynskey, 2015; Svantesson, 2016; Voigt, 2017; Lenaerts, 2019)[23]. In a second pronunciation: Schrems II (Murray, 2017; Diker Vanberg, Maunick, 2018; Tambou, 2018; Dhont, 2019; Chander, 2020; Christakis, 2020; Flett, Wilson, Clover, 2020; Simon, 2020; Tracol, 2020; Voss, 2020; Liss, Peloquin, Barnes, Bierer, 2021)[24], the CJEU declared the implementing

23See inter alias: CJEU, joined cases C-362/14 and C-362/14, Maximilian Schrems v. Data Protection Commissioner-Digital Rights Ireland Ltd of 6 October 2015, ECLI:EU:C:2015:650, published in the electronic Reports of the cases. See also in argument the next cases: C-288/12, Commission v. Hungary of 8 April 2014, ECLI:EU:C:2014:237, published in the electronic Reports of the cases. C-614/10, Commission V. Austria of 16 October 2012, ECLI:EU:C:2012:631, published in the electronic Reports of the cases. joined cases C-92/09 and C-93/09, Volker Volker und Markus und Markus Schecke GbR, Hartmut Eifert v. Land Hessen of 9 November 2010, ECLI:EU:C:2010:662, I-11063. C-28/08, Commission v. The Bavarian Lager Co. Ltd of 29 June 2010, ECLI:EU:C:2010:378, I-06055. C-524/06, Heinz Huber v. Germany of 16 December 2008, ECLI:EU:C:2008:724, I-09795. C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU of 29 January 2008, ECLI:EU:C:2008:54, I-00271. joined cases C-317/04 and C-318/04, European Parliament v. Council of European Union and European Parliament v. Commission of 30 May 2006, ECLI:EU:C:2006:189, I-02457. C-131/12, "Google Spain", Google Inc./Agencia Española de Protección de Datos, (AEPD) and Mario Costeja González", ECLI:EU:C:2006:189, I-02457. C-230/14, Weltimmo of 1st October 2015, ECLI:EU:C:2015:634. C-673/17, Planet49 of 21 March 2019, ECLI:EU:C:2019:246, published in the electronic Reports of the cases.

24CJEU, joined cases C-92/09 and C-93/09, Volker and M. Schecke and Eifert, of 9 November 2010, ECLI:EU:C:2010:662, I-11063, para. 48; C-291/12, Schwartz of 17 October 2013, ECLI:EU:C:2013:670, published in the electronic Reports of the cases, par. 33; joined cases C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk and Others of 20 May 2003, ECLI:EU:C:2003:294, I-04989, parr. 74-75; joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and others of 8 April 2014, ECLI:EU:C:2014:238, published in the eletronic Reports of the cases, parr. 33 and 36; opinion 1/15 of 26 July 2017, ECLI:EU:C:2017:592, published in the electronic Reports of the cases, parr. 124 and 126. C-311/18, Facebook Ireland and Schrems (Schrems II) of 16 July 2020, ECLI:EU:C:2020:559, not yet published.

decision, i.e. the decision privacy Shield 2016/1250 (Alkiş-Tümtürk, 2022)[25], incompatible with the Regulation 2016/278 and in collaboration with Articles 7, 8 and 52 of the Charter for the Fundamental Rights of the European Union (CFREU) for the principle of proportionality (Cardonnel, Rosas, Wahl, 2012; Peers, Hervey, Kenner, Ward, 2014; Von Der Groeben, Schwarze, Hatje, 2015; Stern, Sachs, 2016; Tinière, Vial, 2020; Peers and others, 2021; Ripol Carulla, Ligartemendia Uceizabarrena, 2022). The CJEU, in the Digital Rights Ireland Ltd[26] case, based its assessment on Directive 2006/24/EC and Articles 7 and 8 CFREU on proportionality's principle (Ripol Carulla, Ligartemendia Uceizabarrena, 2022). It was found that the memorization of data relating to communication traffic and location made it possible to draw conclusions on relevant aspects of the life of individuals exceeding the strictly necessary limits for the achievement of the objectives set by the European legislator.

Furthermore, according to the Schrems II case it was found:

> "(...) that the Commission decision, like the previous one 2000/520, which allowed the transfer of data between the EU and the US on the basis of the Safe Harbor Principles (...) sanctioned the primacy of national security needs over the principles established by the Privacy Shield and placed to protect the fundamental rights of the persons whose personal data were transferred, without providing for any limits or guarantees of protection for the

25Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection afforded by the EU-US Privacy Shield regime [notified under number C(2016) 4176], in OJ EU, L 207 of 1 August 2016, p. 1ss.

26CJEU, joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung and others of 8 April 2014, ECLI:EU:C:2014:238, published in the electronic Reports of the cases.

interested parties (...)" (Araùjo, 2015; Flor, 2021)[27].

The legal basis was the adequacy decision of the EC in relation to personal data which could resort to the instruments of Regulation 2016/278 and its related articles, namely 46 and following. Its applicability is residual[28] and, as can be seen in practice, under various controversial conditions[29]. As an alternative we have the contractual clauses and the binding corporate rules. These are types of rules that according to the European Data Protection Committee constitute:

> "(...) a valid legal basis only on the basis of the outcome of an assessment of the conduct by the exporter taking into account the circumstances of the transfers and the measures supplements that may be implemented (...). It is a valid decision, however, it is not clear how for the Court a private instrument, which undoubtedly are the additional measures, (does not bind the State of destination) can guarantee adequate protection pursuant to the GDPR (...)" (Voss, 2020)[30].

Among the first in Europe we note the Austrian data protection authority (Datenschutzbehörde or DSB), which in a decision published

---

27Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection offered by the principles of safe harbor and the related "Frequently asked questions" (FAQ) on privacy issues published by the United States Department of Commerce, 25 August 2000, OJ L. 215/7. The agreement was considered valid with the European Commission decision 2000/520/EC of 26 July 2000.

28As reaffirmed by the European Data Protection Board in its Guidelines 2/2018 on the derogations referred to in Article 49 of Regulation 2016/679, 25 May 2018.

29Art. 49.1 GDPR.

30The category of technical google also includes Google Analytics which allows you to observe, in real time, the movements of users on a given website. Google Analytics operate through JavaScript tags which are executed in the site's source code and which set cookies on browsers to collect and process personal data, sometimes even sensitive ones.

on 13 January 2022[31] asserted that Google Analytics transmits personal data, referable to identified or "identifiable" interested parties pursuant to Article 4.1 of the GDPR, such as inter alia unique identifiers, IP addresses and browser parameters. The Austrian Supervisory Authority also concluded that neither the standard contractual clauses nor the envisaged additional measures offered a sufficient level of protection in this case because the data stored by Google, despite the use of encryption technologies, is subject to surveillance by agencies of US intelligence. Under section 702 of the Foreign Intelligence Surveillance Act Google is required to grant access to or release imported data that is in its possession, custody or control and this obligation may also expressly apply to the cryptographic key without which such data they cannot be read. The Google Analytics tool (at least in the version of 14 August 2020) is therefore not compliant with the requirements of Chapter V of the GDPR since it does not guarantee an adequate level of protection of the data transmitted pursuant to Article 44 of the same Regulation[32]. In the same context, it should be noted that the corresponding French authority, the Commission *nationale de l'informatique et des libertés* (CNIL) has taken a position stating that the additional measures adopted by Google "*ne suffisent pas à exclure la possibilité d'accès des services de renseignements américains à ces données* (...)"[33]. The CNIL also declared the illegality of Google Analytics for

31https://noyb.eu/sites/default/files/2022-01/E-DSB%20%20Google%20Analytics_EN_bk.pdf.
32https://noyb.eu/sites/default/files/2022-01/E-DSB%20%20Google%20Analytics_EN_bk.pdf.
33CNIL, Mise en demeure anonymisée-Google analytics, 10 February 2022. https://www.cnil.fr/sites/default/files/atoms/files/med_google_analytics_anonymisee.pdf.

violation of the GDPR.
The European Data Protection Supervisor had censured the European Parliament for having allowed Google Analytics and the Stripe payment platform, through a web portal dedicated to the Covid tests of the parliamentarians themselves, to transfer the data of its employees to the United States, contrary to the requirements of Regulation 2018/1725[34].
Google immediately (since March 2022) announced the new version of Google Analytics where compared to previous one it will not make use of the registration and storage of information on the IP address of European users as a mechanism for monitoring and analysis, thus limiting the possible transfers of data associated with such use[35]. As a consequence also we have the signing on 25 March 2022 of the Trans-Atlantic Data Privacy Framework (TADPF) between the EU and the US. This is a related "in principle" agreement, where its purpose is to regulate cooperation between the US and the EU in operations on personal data that provide for the transfer of the same between the two parties. In the words of the President of the Commission Ursula Von Der Leyen, it will allow "predictable and trustworthy data flows" between the Union and the United States on the basis of a new balance between security and rights to privacy and the protection of personal data[36]. The first step to strengthen privacy was taken on 7 October 2022

34Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No. 45/2001 and the decision n. 1247/2002/EC (Text relevant for the purposes of the EEA).
35https://blog.google/products/marketingplatform/analytics/prepare-for-future-with-google-analytics-4/
36European Commission, Statement by President von der Leyen with US President Biden,

through the signing by US President Joseph R. Biden Jr. of the "Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities"[37]; following on 13 December 2022 the related proposal by the EU Commission for a new adequacy decision to be adopted against the USA itself, where:

> "(...) the United States have undertaken to implement reforms to strengthen privacy and civil liberties of individuals in the context of intelligence activities and, even more specifically, to ensure that such activities are necessary and proportionate to the pursuit of well-defined national security objectives, as well as to establish appropriate redress and oversight mechanisms. Similar commitments would then materialize in the adoption of an Executive Order, i.e. a provision by the US President, which would have represented the basis of the subsequent assessment of adequacy of the Commission (...)" (Ruschemeier, 2022).

The TADPF predicts that data:

> "(...) will be able to flow freely and securely between participating companies in the European Union and the United States, based on new rules that will limit access to data by US intelligence only in cases where access is necessary and proportionate in order to protect national security (...)"[38](Derave, Genicot, Hetmanska, 2022).

As far as intelligence agencies are concerned, they will be called upon to adopt procedures to ensure effective control of privacy and compliance with civil liberties rules. US companies that process

---

Bruxelles, 25 March 2022, p. 1.

37https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/11/executive-order-on-prohibiting-certain-imports-exports-and-new-investment-with-respect-to-continued-russian-federation-aggression/

38https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087 and from United States see also in argument: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

personal data from the EU will instead have to self-certify their adherence to the Privacy Shield principles through the US Department of Commerce (Flor, 2021)[39]. Within this context, it is envisaged that a related redress mechanism of a multi-level nature will be created by the US, which may include an independent data protection review tribunal to which residents of the EU will also be able to appeal.

The TADPF is not yet operational and the production and accuracy of the relevant legal acts is required to become operational. From the US a relative executive order is needed on the matter and after that the EC must adopt it together with a new adequacy decision as a legal basis for the transfer of data to the US. We cannot yet clearly and precisely assess this legal position and what it will really bring after the Privacy Shield. Perhaps it would be appropriate to address the inadequacies of the US privacy framework by highlighting as a privacy statement the sentence of the Supreme Court in the FBI v. Fazaga[40] case, who confirmed that "(...) the executive order does not appear to be a suitable instrument (...)". Due to the invalidity of the CJEU, it would also be necessary for the Congress to proceed by legislative means to a broader and more organic reform in the sector under discussion, needing many months of implementation (Manfreda, 2022)[41].

THE E.PRIVACY REGULATION

39https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

40Supreme Court of the United States, Federal Bureau of Investigation et al. v. Fazaga et al. Certiorari to the United States Court of Appeals for the Ninth Circuit, 4 March 2022.

41According to Manfreda: "(...) USA is unique among the world's leading countries in that it lacks an umbrella privacy legislation and a governmental authority, who would be responsible for protecting privacy of personal information (...)".

As we have predicted, internet cookies are also a topic of discussion of the ePrivacy regulation with the main objective of regulating the processing of electronic communication data by verifying the supply, use of services and e-communication in a uniform and correct way in all Member States of the Union replacing thus the old ePrivacy directive. The current directive does not apply to electronic communications services offered by providers operating on the internet. The regulation proposal, on the other hand, is applicable to all types of data controllers, also reaching the scope of application to equivalent services from a functional point of view, including the so-called Over The Top (OTT) services.

The regulation began its formation on a EU proposal of January 2017[42]. Its hard core, according to the ideas of the lobby, was to weaken the more innovative parts of the text, oriented towards greater user protection final[43]. The Council had come to talk about the start of inter-institutional trilogues only in February 2021 (Danielle, 2023)[44].

The novelty was the new text that signals the applicability not only to

42European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on privacy and electronic communications), Brussels, 10.01.2017 COM(2017) 10 final 2017/0003 (COD).

43"(...) (Google has) been successful in slowing down and delaying the [ePrivacy Regulation] process and have been working behind the scenes hand in hand with the other companies]" (cfr. https://videoweek.com/2022/03/29/can-eprivacy-come-back-from-the-dead/

44Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)-Mandate for negotiations with EP, Brussels, 10 February 2021 (OR. en) 6087/21.

internet cookies but also to other similar identifiers. Users will be able to limit the entire set of identifiers through the settings of the navigation program, i.e. the browser. Internet cookies have thus represented one of the points of greatest friction and discussion given that the identification of the conditions of lawfulness for the processing of data through them goes beyond simple consent. It is understood that the use of internet cookies is prohibited unless the specific exceptions listed in Article 8. The types of internet cookies do not require the consent of the end user and appear as technically necessary for the purpose of producing aggregate statistics and providing a more specific service that requires the end user to provide an electronic communication service. It is expected that users have given their consent to the processing of data and remember the possibility of withdrawing consent at periodic intervals that do not exceed the 12 months that the treatment lasts.

The Council told us about the use of cookie walls, i.e. binding and technical mechanisms, the so-called take it or leave it where the user is obliged and without an alternative to express its consent regarding their receipt and of other tools tracking, under penalty of being unable to access the site. Consent obtained within the framework of the ePrivacy regulation is required, which has the same meaning governed by the GDPR and must, among other things, be expressed where the European Data Protection Board had considered cookie walls to be incompatible with European rules[45]. Cookie walls can also be used by

45According to the opinion expressed by the European Committee on 25 May 2018, Statement of the European Data Protection Board on the review of the ePrivacy regulation and its impact on the protection of natural persons with regard to the privacy and confidentiality of their communications, p 3), "(...) the need to obtain freely expressed consent will prevent service providers from imposing cookie walls on their

vendors as a GDPR requirement for consent[46]. As an alternative service we can consider the paid version without internet cookies. The consent of internet cookies can be granted through the settings of the navigation program, i.e. through the use of user lists that are configured for one or more suppliers[47]. Consent declares to the end user to prevail over that expressed through the settings of the relative use of the browser. Thus a step backwards is signaled which respects what has been proposed by the EC. Already in the first draft of the ePrivacy regulation, its compliance with the principle of privacy by design[48] was envisaged, where the default browser settings were of a general nature and positioned to give maximum confidentiality resulting of independently excluding third-party cookies parts[49].

The processing of metadata is connected and linked with internet cookies in relation to electronic communications. Metadata, i.e. data on data, are those that give information on the place, time and recipient of the communication and can derive from the use of other data that represent the main survey content used by the user. Metadata seem

---

users". A general opinion against cookie walls was also expressed by the Italian Guarantor, who considered them to be in contrast with the requirement of the "freedom" of consent pursuant to art. 4.11 GDPR without prejudice however to "the hypothesis to be verified on a case-by-case basis in which the site owner offers the interested party the possibility of accessing an equivalent content or service without giving his consent to the installation and use of cookies or other tracking tools (...)" (see Cookie Guidelines, p. 9).

46Council preamble 20(aaaa) of the text as approved by the Council in February 2021.

47Council preamble 20(a) of the text as approved by the Council in February 2021.

48Art. 25.2 GDPR, where it is established that: "(...) the data controller implements adequate technical and organizational measures to ensure that, by default, only the personal data necessary for each specific purpose of the processing are processed. This obligation applies to the amount of personal data collected, the extent of the processing, the retention period and accessibility (...)".

49Art. 20(a) GDPR.

indeterminate and generic therefore we can speak of the processing of data and electronic communications without consent[50]. Thus the risk remains of a lowering of the level of data protection which was guaranteed by the ePrivacy Directive[51].

CONFLICT BETWEEN PRIVACY AND NATIONAL SECURITY

It is obvious that a relative problem has arisen concerning the possibility of overcoming the relationship, namely the connection

50Art. 6b affirms that: "(...) (a) it is necessary for the purposes of network management or network optimisation, or to meet technical quality of service requirements pursuant to Directive (EU) 2018/1972 or Regulation (EU) 2015/2120; or (b) it is necessary for the performance of an electronic communications service contract to which the end-user is party, or if necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or (c) the end-user concerned has given consent to the processing of communications metadata for one or more specified purposes; or (d) it is necessary in order to protect the vital interest of a natural person; or (e) in relation to metadata that constitute location data, it is necessary for scientific or historical research purposes or statistical purposes (...)", (pp. 54-55).

51According to the European Data Protection Board: "(...) the approach of the proposed regulation (...) provides for broad prohibitions, limited exceptions and the use of consent. Consequently, the ePrivacy Regulation should not provide for the possibility of processing the contents and metadata of electronic communications on the basis of less stringent legal prerequisites, such as for example the so-called "legitimate interests", which go beyond what is necessary for the provision of an electronic communications service. The ePrivacy Regulation should also not allow electronic communications metadata to be processed for the performance of a contract, which means that there should be no exceptions based on the general purpose of the performance of a contract, as the Regulation establishes which specific processing is legitimate for this purpose, for example that for billing purposes (...)". (European Data Protection Board, Declaration of the European Data Protection Board on the review of the ePrivacy regulation and its impact on the protection of natural persons in relation to the privacy and confidentiality of their communications, 25 May 2018, p. 2).

between privacy and state security understood as a conflict of "privacy versus national security" and also evaluating the binomial "privacy with national security" and national and/or EU security.

The lowering of the levels of protection of personal data on the net has as a consequence a margin of maneuver on the part of the law enforcement authorities and the security services. At the same time, on the other side, the same margin could be exploited by cyber-terrorists and cuber-criminals to carry out harmful acts against society. The protection of personal data and its collection without discrimination is a more effective way to protect national security because it allows us to limit the room for maneuver of criminal activities that operate mostly through the network.

The need to protect personal data in conflicts also requires protection of national security. In the past, the Special Rapporteur on Privacy Joseph Cannatacci proposed to overcome the contrast stating in the report published in 2016 that

> "(...) it is not helpful to talk of "privacy vs. security" but rather of "privacy and security" since both privacy and security are desired (...) and both can be taken to be enabling rights rather than ends in themselves (...)"[52].

This position finds a foundation not only on a practical level but also in relation to cases of cyber-terrorism both on a theoretical and doctrinal level. The right to privacy and national security/law enforcement is also based on a paradox. One of the purposes of terrorism is to destroy the rule of law and threaten national security:

> "(...) also by triggering excessive and disproportionate reactions in States, for which they are led to adopt disproportionate and repressive countermeasures of the rights of individuals (...)" (Sottiaux, 2008).

52Council of Human Rights, Report of the Special Rapporteur on the right to privacy, 31st session, 24 November 2016, A/HRC/31/64, par. 24.

States by restricting human rights help to realize the objectives set by the aforementioned terrorists.
This is Sottiaux's position that conceives the question in terms of contrast where on the one hand we protect personal data and on the other we guarantee national security, based on erroneous legal assumptions. It is a trade-off between "privacy and security" where on the one hand it concerns the need to protect national security and, on the other, it leans downwards towards the protection of privacy becoming thus an "obstacle against achieving the most cherished objective (...)"[53]. With this type of conflict, it is necessary to re-evaluate the importance that law, especially that of the EU, assumes in the international legislative system, also including the right to private and family life, the secrecy of correspondence as a means by which the identity of an individual is developed. The right to privacy, in its broadest conception, is based on ex Article 8 of the European Convention of Human Rights (ECHR) (Sudre, 2021; Villiger, 2023) and ex Article 17 of the Covenant on civil and political rights. The latter is "instrumental" and fundamental for the protection of other rights, such as the right for every individual to manifest and develop his own personality (Schoeman, 1984; Cudd, Navin, 2018). Protecting this type of right also allows respect for the rule of law.
The "privacy/national security" debate can be found in the various legislative and jurisprudential systems, analyzed both at an international and European level, showing in theory and in practice a positive tendency to recognize a fundamental value of the right to the protection of personal data and to judge all any limitations always in

53Council of Human Rights, Report of the Special Rapporteur on the right to privacy, 31st session, 24 November 2016, A/HRC/31/64, par. 24.

the light of the principles of proportionality, necessity and legitimacy. In this regard, the Advocate General Saugmandsgaard Øe stated in his opinion in the Tele2 Sverige AB case that:

> "(...) the requirement of proportionality stricto sensu implies weighing the advantages resulting from a measure in terms of the legitimate objective pursued against the disadvantages it causes in terms of the fundamental rights enshrined in a democratic society. This particular requirement therefore opens a debate about the values that must prevail in a democratic society and, ultimately, about what kind of society we wish to live in (...)"[54].

CONCLUDING REMARKS

The French CNIL has already questioned and fined through two measures both Google and Youtube on the one hand and Facebook based on violations of the European legislation relating to internet cookies on the other[55]. In particular, the cookie banners presented on the Google, Facebook and YouTube sites required only a simple click to accept them or five seconds for one's refusal. Thus they can induce internet users to accept the markers without a precise and clear understanding of the implications connected to the relative choice. According to the French guarantor the aforementioned companies and

54CJEU, joined cases: C-203/15 and C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson e altri of 21 December 2016, ECLI:EU:C:2016:970, published in the electronic Reports of the cases.

55CNIL, Délibération de la formation restreinte n° SAN-2021-023 du 31 décembre 2021 concernant les sociétés Google Llc et Google Ireland Limited, published 6 January 2022: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840062. CNIL, Délibération de la formation restreinte n°SAN-2021-024 du 31décembre 2021 concernant la société Facebook Ireland Limited, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840532.

related banners, while allowing you to choose between accepting and rejecting cookies, nonetheless use methods "*(...) par lesquelles ce refus peut être exprimé [...] [qui] biaise l'expression du choix en faveur du consentement de façon à altérer la liberté de choix" (...)*"[56].

The behaviors can be qualified as "dark patterns", i.e. interfaces aimed at directing users, thus exploiting their cognitive biases and as a solution favorable to the owner of an online service (Brignull, 2018; Gray, Kou, Battles, Hoggatt, Toombs, 2018; Nouwens, Liccardi, Veale, Karger, Kagal, 2020; Soe, Nordberg, Guribye, Slavkovik, 2020; Kollmer, Eckhardt, 2022)[57]. As points of discussion and with the relative conclusions are: i) a minority of Internet users faced with cookie banners with dark patterns that reach the second level to deny the relative consent and ii) a situation that dates back a long time ago and does not finds a solution especially following the entry into force of the GDPR (Utz, Degeling, Fahl, Schaub, Arbor, Holz, 2019; Santos, Bielova, Matte, 2020; Kulyk, Gerber, Hilt, Volkamer, 2020; Bollinger, Kubicek, Cotrini, Basin, 2021; Lancers, 2022).

On the one hand we find the need of the majority of Internet users to be able to navigate quickly and without hindrances and on the other hand the false perceptions induced by the dark patterns that characterize cookie banners, i.e. the consequences of not giving consent to internet cookies. The ePrivacy regulation must reduce the amount of notifications that users are exposed by eliminating the need for consent for necessary or harmless internet cookies (Graßl,

56CNIL, Délibération de la formation restreinte n°SAN-2021-024 du 31décembre 2021 concernant la société Facebook Ireland Limited, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840532.

57EDPB, Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them, Version 1.0, 14 March 2022.

Schraffenberger, Zuidereen Borgesius, Buijzen, 2021)[58]. Providing whitelists that are not mandatory should reduce consent fatigue.
The absence of real changes in the behavior of many owners lead to substantial changes introduced over time to European cookie law due to the guarantee of greater protection for end users. The non-fulfilment and circumvention of the obligations imposed by EU law have been mainly attributed to a problem of insufficient enforcement (Bollinger, Kubicek, Cotrini, Basin, 2021)[59]. This problem puts us into question and trouble due to missing national data protection regulations. The particularly pervasive information asymmetries and market power found in many data markets undermine the role of markets, torts, and regulatory enforcement as mechanisms to ensure legal compliance (Lancieri, 2022). The recent and various types of initiatives both on a regulatory level such as the guidelines on internet cookies and on decision-making seem to have imposed many steps forward but also backwards given that on various topics security and data protection continues to be a topic with many gaps especially for large and small companies that will have to adapt to avoid high-level fines.
According to Liakopoulos:

58"(...) the upcoming ePrivacy Regulation of the EU should limit the number of cookie consent requests peopleare confronted with (...)".

59"Many websites do not give users a choice over which cookies are collected, despite the GDPR and ePrivacy Directive requirements. Multiple prior studies report on this, and we contribute to this analysis by showing that even from the websites providing choices, the vast majority, namely 94.7%, contain at least one potential violation. This situation cannot be resolved through new regulations alone, such as the planned ePrivacy Regulation, as it is mostly enforcement that is significantly lacking behind (...) all in all, the extent to which the GDPR bans dark patterns must become clear in case law and enforcement actions by Data Protection Authorities (...)" .

> "(...) the profitable interweaving between aware and timely regulatory intervention, the proactive attitude of the data controllers, and the empowerment of digital users will increasingly constitute an essential factor for sustainable and intelligent growth, especially with reference to the increasingly broader areas of application and use of personal data. In the absence of this combined action, on the contrary, it is reasonable to expect the perpetuation of the risk that the ever more invasive use of new technologies, from an instrument of growth and development of the community based on the fertile sharing of information and knowledge, will turn into a vehicle of limitation of personal freedoms and fundamental rights, transforming the much desired digital society into a strongly dystopian one (...)" (Liakopoulos, 2019).

Finally, international documents and meetings within the European Union are always a good starting point for a universal discussion on this type of issue. If the same means of communication (Oster, 2016) will do their part to favor it by guaranteeing the independence and pluralism of information, equally emphasized in state declarations there will be absolutely everyone's commitment to overcome the digital divide with cooperation and dialogue in a non-formal but substantial framework of peace and democracy. We are witnessing a front page which often demonstrates an excessive permeability towards a global administration which legitimizes the false theses adopted to justify wars, to indirectly reveal decisions entrusted to events so delicate that if they were otherwise they would not be questionable, but wrapping them in reassuring opaque fabric of embedded information, where other information professionals have reclaimed and painstakingly conquered a space of autonomy and tearing up that network, have contested attempts to deny certain crimes, giving strength and visibility to those who still stubbornly seek to reason with the Internet off (Liakopoulos, 2019).

REFERENCES

Alkiş-Tümtürk, A. (2022). Uncertain future of transatlantic data flows. Will the United States ever achieve the "adequate level" of data protection? *Hungarian Journal of Legal Studies, 63 (3).*

Araùjo, A.M.R. (2015). The right to data protection and the commissions' adequacy decision. *Unio EU Law Journal, 1 (1),* 78ss.

Bollinger, D., Kubicek, K., Cotrini, C., Basin, D. (2021). *Automating cookie consent and GDPR violation detection.* ETH Zurich, 2021. https://karelkubicek.github.io/assets/pdf/Automating_Cookie_Consent_and_GDPR_Violation_Detection

Brignull, H. (2018). What are dark patterns? https://darkpatterns.org

Burri, M., Schär, R. (2016). The reform of the EU data protection framework: Outlining key changes and assessing their fitness for a data-driven economy. *Journal of Information Policy, 6,* 482ss.

Cardonnel, P., Rosas, A., Wahl, N. (2012). *Media of constitutionalising the EU judicial system. Essays in honour of Pernilla Lindh.* Oxford University Press, Oxford, 292ss.

Caruana, M. (2017). The reform at the EU data protection framework in the context of the political and criminal justice sector: Harmonisation, scope, oversight and enforcement. *International Review of Law, Computers and Technology, 31.*

Chander, A. (2020). Is data localization a solution for Schrems II?. *Journal of International Economic Law, 23,* 772ss.

Christakis, T. (2020, July, 21). After Schrems II: Uncertainties on the legal basis for data transfers and constitutional implications for Europe. *Europeanlawblog.eu*: https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-

constitutional-implications-for-europe/
CNIL"s (2019), *6th Innovation and Foresight Report "Shaping Choices in the Digital World, "From dark patterns to data protection: the influence of UX/UI design on user empowerment"*: https://linc.cnil.fr/fr/ip-report-shaping-choices-digital-world.
Cudd, A.E., Navin, M.C. (2018). *Core concepts and contemporary issues in privacy.* ed. Springer, Berlin, pp. 61ss.
Danielle, M., (2023, February, 23). *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, EUAA: European Union Agency for Asylum.* Retrieved from REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL | Policy Commons
De Hert, P., Papakonstantinou, V. (2012). The proposed data protection Regulation replacing Directive 95/46/EC. A sound system for the protection of individuals. *Computer Law & Security Review, 28 (2),* 132ss.
Deac, A. (2018). Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of these data. *Perspectives of Law and Public Administration, 7 (2),* 152ss.
Derave, C., Genicot, N., Hetmanska, N. (2022). The risks of trustworthy artificial intelligence: The case of the European travel information and authorisation system. *European Journal of Risk Regulation, 13(3),* 389-420.
Dhont, J.H. (2019). Schrems II. The EU adequacy regime in existential crisis?. *Maastricht Journal of European and Comparative Law, 5,* 598ss.
Diker Vanberg, A., Maunick, M. (2018). Data protection in the UK post-Brexit: The only certainty is uncertainty. *International Review of Law, Computers, and Technology, 32,* 191-193.
Donohue, L.K. (2023). Surveillance, State secrets and the future of constitutional rights. *Supreme Court Review* (forthcoming).

Edwards, L. (2018). Data protection and e-Privacy: From spam and cookies to big data, machine learning and profiling. In L. Edwards (ed.). *Law, policy and the internet.* Bloomsbury Publishing, New York. 119, 126ss
Edwards, L. (2019). *Law policy and the internet*. Hart Publishing, London, New York, New Delhi, Sydney.
Feiler, L. (2010). The legality of the Data Retention Directive in light of the fundamental rights to privacy and data protection. *European Journal of Law and Technology, 1 (3).*
Flett, E., Wilson, J., Clover, J. (2020). Schrems strikes again: EU-US privacy Shield suffers same fate as its predecessor. *Computer and Telecommunication Law Review, 6,* 162ss.
Flor, A. (2021). The impact of Schrems II: Next steps for U.S. data privacy law. *Notre Dame Law Review, 96,* 2039ss.
Glass, A. (2010). Privacy and Law. In H., Blatterer, P., Johnson, M.R., Markus, (eds) *Modern privacy.* Palgrave Macmillan, London.
Graßl, P., Schraffenberger, H., Zuidereen Borgesius, F.R., Buijzen, M. (2021). Dark and bright patterns in cookie consent requests. *Journal of Digital Social Research, 3 (1),* 28.
Gray, C.M., Kou, Y., Battles, K., Hoggatt, J., Toombs, A.L. (2018). The dark (patterns) side of UX design. *Proceedings of the CHI Conference on Human Factors in Computing Systems ACM,* New York, USA, 2018.
Hallinan, D., Leenes, R., Gutwirth, S. (2020). *Data protection and privacy. Data protection and democracy.* Bloomsbury Publishing, New York.
Kollmer, T., Eckhardt, A. (2022). Dark Patterns. *Business & Information Systems Engineering, 64*
Kulyk, O., Gerber, N., Hilt, A., Volkamer, M. (2020). Has the GDPR hype affected users' reaction to cookie disclaimers?. *Journal of Cybersecurity*, 6 (1), 4ss.

Lancieri, F. (2022). Narrowing data protection's enforcement gap. *Maine Law Review, 74 (1)*
Lenaerts, K (2019). Limits on limitations: The essence of fundamental rights in the EU. *German Law Journal, 20,* 773ss.
Liakopoulos, D. (2019). Regulation (EU) 2016/679 on the protection of personal data in light of the "Cambridge Analytica" affair. *E-Journal of Law. An indipendent law Journal, 5 (1)*
Liakopoulos, D. (2020). The protection of personal data according to CJEU and ECtHR jurisprudences. *Journal of Digital and Data Law, 6,* 135-191.
Liss, J., Peloquin, D., Barnes, M., Bierer B.E. (2021). Demystifying Schrems II for the cross-border transfer of clinical research data. *Journal of Law and the Biosciences*, 8, (2).
Lynskey, O. (2015). Control over personal data in a digital age: Google Spain v AEPD and Mario Costeja Gonzalez. *Modern Law Review, 78 (3),* 522-534.
Manfreda, D. (2022). GDPR and data transfer: Focusing on data flow between the EU and USA before and after the Schrems II decision. *European Union Law Working Papers No. 62,* 16ss.
Mantelero, A. (2012). Cloud computing, trans-border data flows and the European Directive 95/46/EC: Applicable law and task distribution. *European Journal for Law and Technology, 3 (2).*
Murray, A.D. (2017). Data transfers between the EU and the UK post Brexit?. *International Data Privacy Law, 7,* 158-162.
Nouwens, M., Liccardi, N., Veale, M., Karger, D., Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. *Proceedings of CHI '20 CHI Conference on Human Factors in Computing Systems,* April 25-30, 2020, Honolulu, HI, USA.

Oster, J. (2016). *European and international media law.* Cambridge University Press, Cambridge, 368ss.
Peers, S. et al. (eds.) (2021). *The EU Charter of Fundamental Rights, A Commentary.* Hart Publishing, Nomos, C.H. Beck, Oxford & Oregon, Portland.
Peers, S., Hervey, T., Kenner, J., Ward, A. (2014). *The EU Charter of Fundamental rights: A commentary*. Oxford University Press, Oxford, 1414ss.
Purtova, N. (2018). Between the GDPR and the police directive: navigating through the maze of information sharing in public-private partnerships. *International Data Privacy Law, 8,* 64ss.
Ripol Carulla, S., Ligartemendia Uceizabarrena, J.I. (2022). *La Carta de derechos fundamentales de la Uniòn Europea.* Marcial Pons, Madrid.
Ruschemeier, H. (2022, November 14). *Nothing new in the west? The executive order on US surveillance activities and the GDPR*, in *European Law Blog*: https://europeanlawblog.eu/2022/11/14/nothing-new-in-the-west-the-executive-order-on-us-surveillance-activities-and-the-gdpr/
Santos, C., Bielova, N., Matte, C. (2020). Are cookie banners indeed compliant with the law?: Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. *Technology and Regulation,* 94ss.
Sauter, W. (2014). *Public services in European Union law.* Cambridge University Press, Cambridge.
Scheck, D. (2012). *Economic and social integration. The challenge for EU constitutional law.* Edward Elgar Publishers, Cheltneham.
Schoeman, F. (1984). Privacy: Philosophical dimensions. *American Philosophical Quarterly, 21,* 202ss.
Schwarz, J. (2001, September, 4). Giving the web a memory cost its users

privacy. *New York Times,* http://www.nytimes.com/2001/09/04/technology/04Cook.html.
Shah, R.C., Kesan, J.P. (2004). Deconstructing code. *Yale Journal of Law and Technology, 25,* 278ss.
Simon, D. (2020). Coup de tonnerre dans le monde du numérique. *Europe, 8-9,* pp. 7ss.
Soe, T.H., Nordberg, O.E., Guribye, F., Slavkovik, M. (2020, June, 20). Circumvention by design-dark patterns in cookie consents foronline news outlets, NordiCHI'20: *Proceedings of the 11th Nordic Conference in human-computer interaction. Shaping expriences, shaping society*
Sottiaux, S. (2008). *Terrorism and the limitations of rights, the ECHR, the US Constitution.* Hart Publishing, Oxford & Oregon, Portland, 5ss.
Stern, K., Sachs, M. (2016). *Europäische Grundrecht Charta.* ed. C.H. Beck, München, 756ss.
Sudre, F. (2021). *La Convention europèennes des droits de l'homme.* PUF, Paris
Svantesson, D. (2016). The CJEU's Weltimmo data privacy ruling: Lost in the data privacy turmoil, yet so very important case C-230/14, Weltimmo, EU:C:2015:639. *Maastricht Journal of European and Comparative Law, 2,* 334ss.
Tambou, O. (2018). Opinion 1/15 on the EU-Canada Passenger Name Record (PNR) Agreement: PNR agreements need to be compatible with EU fundamental rights. *European Foreign Affairs Review, 23 (2),* 189ss.
Tinière, R., Vial, C. (2020). *Les dix ans de la Charte des droits fondamentaux e l'Union europèenne.* ed. Larcier, Bruxelles.
Tracol, X. (2020). "Schrems II": The return of the privacy shield. *Computer Law & Security Review, 39,* pp. 4ss.
Turner, C., Johnson, D. (2017). *Global infrastructure networks: The trans-*

national strategy and policy interface. Edward Elgar publishers, Cheltenham.
Utz, C., Degeling, M., Fahl, S., Schaub, F., Arbor, A., Holz, T. (2019, November 11-15). *(Un)informed consent: Studying GDPR consent notices in the field, 019 ACM SIGSAC Conference on Computer and Communications Security (CCS'19).* London, United Kingdom. ACM, New York, NY, USA.
Van Alsenoy, B. (2017a). Liability under EU data protection law: From Directive 95/46 to the General Data Protection Regulation. *Journal of Intellectual Property Information Technology and e-Commerce, 7,* 272ss.
Van Alsenoy, B. (2017b). Reconciling the (extra)territorial reach of the GDPR with public international law. In B. Van Alsenoy, *Data Protection and Privacy under Pressure-Transatlantic tensions, EU surveillance, and big data.* Maklu, Antwerp.
Villiger, M.E. (2023). *Handbook on the European Convention on Human Rights.* ed. Brill, Bruxelles
Voigt, P., Von Dem Bussche, A. (2017). *The European Union General Data Protection Regulation (GDPR): A practical guide.* ed. Springer, Berlin, 23ss.
Von Der Groeben, H., Schwarze, J., Hatje, A. (2015). *Europäisches Unionsrecht.* ed. Nomos, Baden-Baden, 820ss.
Voss, W.G. (2020). Cross-border data flows, the GDPR, and data governance. *Washington International Law Journal, 30 (3),* 485ss
Whitman, J.Q. (2004). The two western cultures of privacy: dignity versus liberty. *Yale Law Journal, 113,* 1152ss.
Wiedemann, K. (2020). The ECJ's decision in "Planet49" (Case C-673/17): A cookie monster or much ado about nothing?. *IIC-International Review of Intellectual Property and Competition Law, 51,* 543-553.
Wulf, A.J., Seizov, O. (2022). Please understand we cannot provide further information: Evaluating content and transparency of GDPR-

mandated AI disclosures. *AI & Society.*